State of North Carolina

Information Resource Management Commission

Requirements
Statewide Security Assessment Project

Version No. PV1

September 24, 2003

Table of Contents

1.0 Background and Objectives

1.1 Project Overview

In response to provisions of North Carolina Session Law 2003-153 (see below), which states that periodic agency security assessments will be performed by the State Chief Information Officer (CIO), the State of North Carolina has initiated a statewide security assessment of all Executive Branch agencies. The assessment process, described in detail in the following sections, is ultimately intended to provide key-decision makers with: 1) a global view of the security status of agencies, and, 2) specific assessment findings in detail sufficient to permit the State to prioritize and budget for required remediation efforts.

> **Section 1. (a)** G.S. 147-33.82 is amended by adding a new section to read:"(e1) The State Chief Information Officer shall assess the ability of each agency to comply with the current security enterprise-wide set of standards established pursuant to this section. The assessment shall include, at a minimum, the rate of compliance with the standards in each agency and an assessment of each agency's security organization, network security architecture, and current expenditures for information technology security. The assessment shall also estimate the cost to implement the security measures needed for agencies to fully comply with the standards. Each agency subject to the standards shall submit information required by the State Chief Information Officer for purposes of this assessment. Not later than May 4, 2004, the Information Resources Management Commission and the State Chief Information Officer shall submit a public report that summarizes the status of the assessment, including the available estimates of additional funding needed to bring agencies into compliance, to the Joint Legislative Commission on Governmental Operations and shall provide updated assessment information by January 15 of each subsequent year."

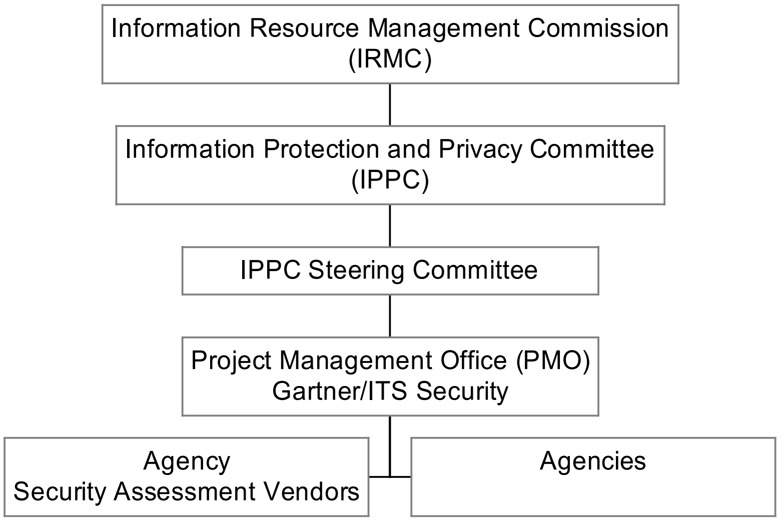
In order to meet the assessment requirements within the timeline specified by state law, the State Chief Information Officer has determined it necessary, as well as prudent, to draw upon the resources and expertise of the private sector. To that end, the State of North Carolina, through a competitive bid process, has developed a list of vendors qualified to conduct the required security assessments of the State's Executive Branch agencies. Vendors selected from this approved vendor list (hereafter referred to as "vendor(s)") will be engaged to conduct security assessments of one or more Executive Branch departments or agencies (hereafter referred to as "agencies"). Vendors will be primarily responsible to conduct thorough and complete agency assessments within the timeframes and budget specified herein.

Security assessments of individual agencies will be conducted under the oversight of the Project Management Office (PMO). The primary roles of the Project Management Office will be to coordinate the overall assessment effort and to review vendors' assessment results for consistency with assessment processes and appropriate diligence. The PMO will be staffed by a team of State ITS security professionals and a team of consultants from Gartner, Inc.. Gartner, which was selected through a previous competitive bidding process, will provide additional project management and assessment process expertise.

The Project Management Office, in turn, will report to a Steering Committee that is comprised of several members of the Information Protection and Privacy Committee (IPPC) and other government officials. The IPPC is a committee of the Information Resource Management Commission. The Information Protection and Privacy Committee develops information technology security and privacy policies, standards and procedures. The Steering Committee will monitor project progress and provide oversight and direction.

The Steering Committee shall report to the full body of the IPPC, which is responsible to the Information Resource Management Commission (IRMC). The IRMC is a statutorily created body that oversees information technology for state government. By statute, it is charged with the State CIO to report the assessment findings to the General Assembly by May 4, 2004. Figure 1 below provides an overview of the project reporting structure.

Figure 1. Security Project Reporting Structure


Information Resource Management Commission (IRMC)
Information Protection and Privacy Committee (IPPC)
IPPC Steering Committee
Project Management Office (PMO) Gartner/ITS Security
Agency Security Assessment Vendors
Agencies

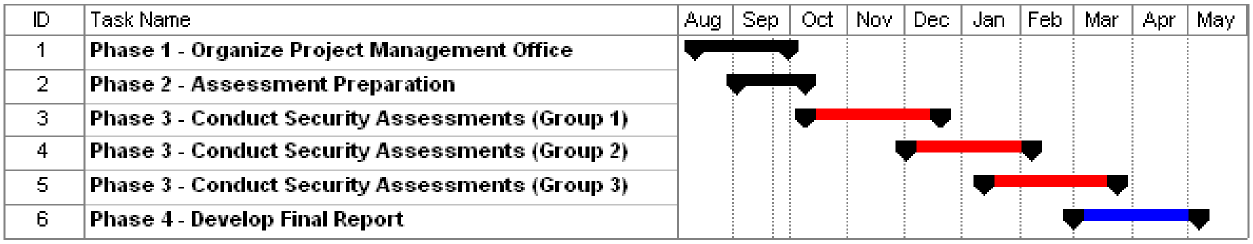
By definition, an assessment is a process of defining, selecting, designing, collecting, analyzing, interpreting, and using information for the purpose of determining how well performance matches baseline standards and expectations. The Project Management Office is currently developing security assessment tools and templates based upon the IS0 17799 standard. These tools and templates will be used by vendors to: 1) evaluate agency compliance with existing security policies and standards, and industry best practices, and, 2) identify areas for improvement for each agency. A matrix identifying the areas of focus for the assessment is included in Appendix A.

In brief, the assessment is intended to determine the sufficiency of agency information security policies, standards, procedures, and guidelines, and to determine the level of compliance with those policies, standards, procedures and guidelines. Although the assessment may involve the review of the implementation of policies, standards, procedures and guidelines on certain key assets, the assessment is intended to provide a holistic view of security management issues from a management perspective, not at the appliance or application level. As such, although vendor assessment teams may conduct eyes-on verification, the assessment is not to be considered a general, or even limited, audit. Furthermore, it should be noted that vulnerability testing, which is under the auspices of the Office of the State Auditor, is beyond the scope of the agency security assessments described in this Requirements Document.

1.2 Project Budget and Schedule

As noted in North Carolina Session Law 2003-153, the State Chief Information Officer must deliver the security assessment report to the Joint Legislative Commission on Governmental Operations by May 4, 2004. In order to meet this requirement, the Project Management Office has developed a project schedule and Work Breakdown Structure (WBS) that details project tasks, task duration, and task dependencies. The PMO will monitor and manage vendor work effort to meet this schedule. Due to the noted deadline, no schedule slip can be accommodated. A summary level view of the project schedule is shown in Figure 2. Specific project activity dates and deadlines are presented in Appendix B.

Figure 2. High Level Project Schedule



ID	Task Name	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May
1	Phase 1 - Organize Project Management Office										
2	Phase 2 - Assessment Preparation										
3	Phase 3 - Conduct Security Assessments (Group 1)										
4	Phase 3 - Conduct Security Assessments (Group 2)										
5	Phase 3 - Conduct Security Assessments (Group 3)										
6	Phase 4 - Develop Final Report										

In addition to the aforementioned time constraint, the security assessment is also constrained by funding. Only a limited amount of funds are available, all of which are allocated for the security assessment project tasks defined by this Requirements Document. Correspondingly, the State has instituted a number of controls and processes to ensure that the statewide security assessment is completed within budget. These controls include: 1) maximum cost ceilings on individual assessment activities and, 2) Project Management Office tracking and management of spend rates against project progress.

Scheduled time and budget caps for vendors to complete agency security assessments are listed in Figure 3.

Figure 3. Assessment Schedule and Work Effort By Agency Type

	Type 1	Type 2	Type 3
Number of Agencies	11	11	3
Fact Finding/Diligence Effort	2 week	2.5 weeks	3 weeks
Findings Development	1 week	1.5 week	2 weeks
Total Time to Complete Assessment *	3 weeks	4 weeks	5 weeks
Hours Cap (per agency)	200	300	400
Note: all times are stated in calendar weeks except Hours Cap			
* Does not include pre-planning and agency debrief activities			

A break down of the estimated number of hours by task is provided in Appendix C.

2.0 Policies, Procedures and Standards

This section describes general State policies, procedures and standards as well as project specific requirements that vendors must follow. Additional information regarding vendor, agency and Project Management Office responsibilities is presented in Sections 3 and 4.

2.1 Conforming to North Carolina Policies

Vendors are responsible for conforming to the policies, procedures and standards of the State Office of Information Technology Services (ITS). This includes but is not limited to policies and procedures for Security and Code of Conduct (e.g., Internet usage, passwords, access to production systems and intellectual property, etc.). Applicable policies, procedures, and standards will be provided during the mandatory vendor training session described in Section 3.

2.2 Vendor Compliance

- Each vendor employee assigned to the project must sign a non-disclosure agreement and successfully pass a background check conducted at the vendor's expense. Copies of the Non-Disclosure Agreement and Background Check Form are included in Appendix D. No waivers will be granted for previous background checks.
- Each vendor employee assigned to the project must attend the mandatory vendor training session described in Section 3. Vendor employees that have not completed the obligatory training will be prohibited from performing any task directly associated with a security assessment activity.
- Vendors are reminded that they will be required to comply with the protection of the intellectual property of other vendors as well as the confidentiality of the State's information as per GS 132 – 6.1(c). Additionally, vendors are prohibited from disclosing any assessment findings or results to any party except: 1) to the Project Management Office as required; 2) to authorized State Office of Information Technology Services management as required; and, 3) to management of the assessed agency during the formal sanctioned debrief. Any unauthorized disclosure of assessment findings or results, including premature disclosure to the assessed agency or to other State agencies, is grounds for immediate removal from the security assessment project.

3.0 Roles and Responsibilities

This section captures general roles and responsibilities for vendors, agencies, and the Project Management Office. Specific roles and responsibilities information on a by-task basis is presented in Section 4.

3.1 Vendor Responsibilities

In addition to responsibilities delineated elsewhere in this document, the vendor shall be responsible for:

- Providing any hardware and software necessary to complete the security assessments.
- Providing all necessary IT-related administrative, managerial and technical resources and staffing necessary to perform its responsibilities and deliver the services described in this document.
- Proper disposition of all State materials upon completion of the project. The vendor shall report such disposition (return to agency, destruction, etc.) to the PMO at project close-out using a form provided by the PMO.
- Directing all questions, concerns and issues to the Project Management Office. Contact information for the PMO is provided in Appendix F.

3.2 Agency Responsibilities

In addition to responsibilities delineated elsewhere in this document, the agency shall be responsible for:

- Making appropriate staff available for the vendor to perform the assessment. The agency also shall provide reasonable access to the technical resources required for the assessment.
- Providing meeting space for conducting security assessments.
- Providing reference information on a timely basis.
- Directing all questions, concerns and issues regarding the assessment process to the Project Management Office. Contact information for the PMO is provided in Appendix F.

3.3 PMO Responsibilities

In addition to responsibilities delineated elsewhere in this document, the Project Management Office shall be responsible for:

- Maintaining the Project Library.
- Providing updates and keeping ITS apprised of project and project status.

- Resolving all vendor and agency questions, or act as a clearinghouse for issues that the PMO staff is unable to resolve. The PMO shall track the status of all inquires and ensure that questions, concerns and issues are resolved in a timely manner.
- Attending meetings and providing communications support as required by ITS.
- Extrapolating results from agency assessments to a statewide basis, if required.

The following table identifies the underlying responsibilities associated with conducting security assessments. An “X” is placed in the column under the party that will be responsible for performing the task. Vendor responsibilities are indicated in the column labeled “Vendor.”

Figure 4. Roles and Responsibility Matrix

Responsibilities	PMO	Vendor	Agency
ASSESSMENT AND MANAGEMENT ACTIVITIES			
1.Manage overall security assessment project	X		
2.Manage assigned agency assessment project work		X	
3.Prepare security assessment tools and templates	X		
4.Prepare assessment scorecard	X		
5.Develop project management tools	X		
6.Develop project schedule and WBS	X		
7.Develop risk management plan	X		
8.Develop Requirements Document	X		
9.Develop billable hour and budget tracking tools	X		
10. Develop deliverables acceptance forms	X		
11. Prioritize agencies and assign vendors to agencies	X		
12. Develop guidelines for agency resource requirements	X		
13. Identify and schedule agency resources			X
14. Gather requested agency data and background information			X
15. Conduct agency assessment via interviews, document reviews, etc.		X	
16. Participate in agency assessment activities		X	X
17. Prepare agency assessment reports to address compliance with existing policies, standards, procedures, guidelines and best practices		X	
18. Develop agency Security Findings Overview		X	
19. Review and accept agency assessments	X		
20. Develop statewide Security Assessment Report	X		

Responsibilities	PMO	Vendor	Agency
REPORTING AND COMMUNICATIONS			
1.Specify the content and purpose of documents and schedule the production of PMO documents	X		
2.Develop Communications Plan	X		
3.Create communications policies/tools	X		
4.Develop project reporting tools	X		
5.Report project progress to ITS and IRMC	X		
6.Complete vendor project reports on or before deadlines		X	
7.Adhere to communications policies		X	
8.Create presentations and briefing materials	X		
9.Participate in designated presentations and meetings	X	X	X
10. Review documentation delivered by agencies	X	X	
11. Review and approve documentation delivered by vendor(s)	X		
12. Preparation of all other project related documentation	X		
13. Develop recommendations to bring agencies into compliance	X		
TRAINING / KNOWLEDGE TRANSFER ACTIVITIES			
1.Develop training materials	X		
2.Provide technical and procedural training for eligible vendors related to the unique skills and processes required to conduct security assessments	X		
3.Participate in vendor training sessions		X	
4.Provide final deliverables to PMO at project closeout		X	
5.Update project library at project closeout	X		

4.0 Process and Tasks

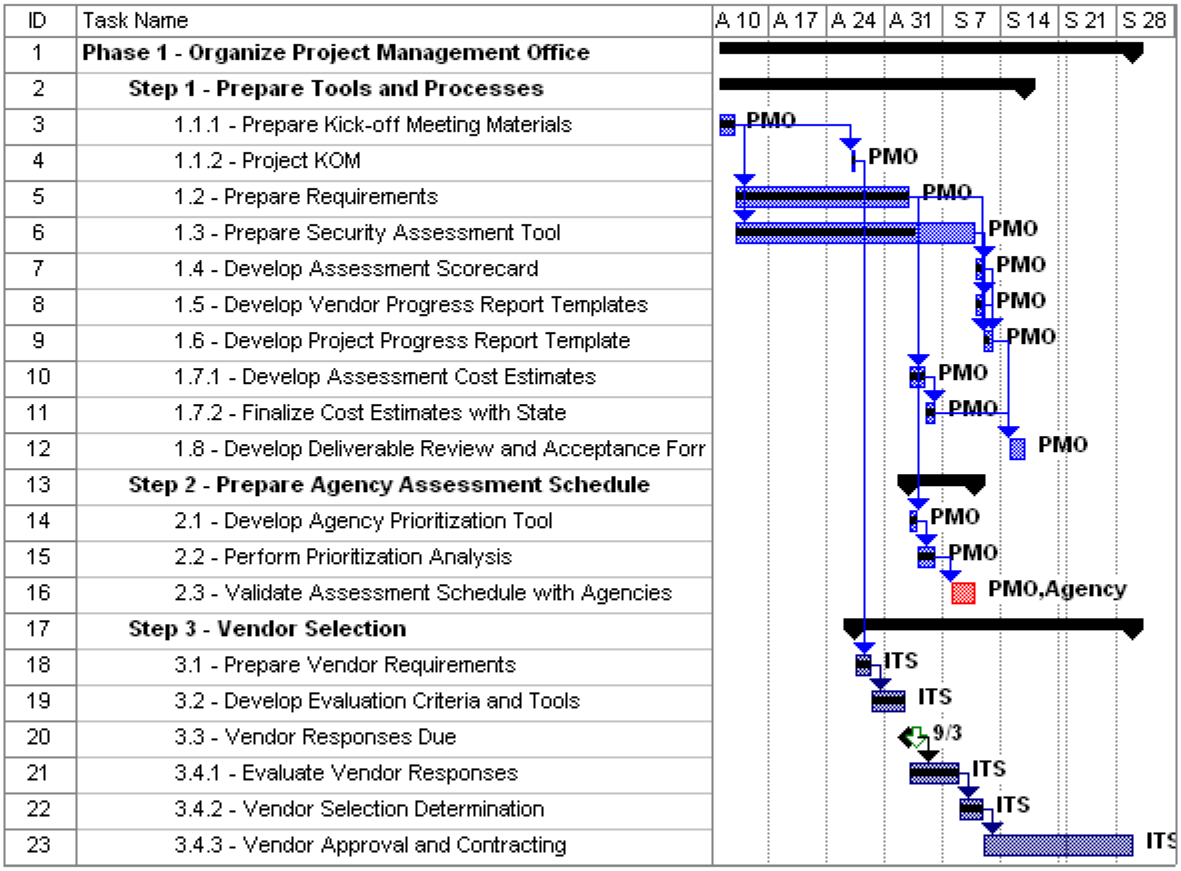
The following section describes the activities and tasks associated with preparing for and actually performing the agency security assessments. Specific Project Management Office, vendor and agency responsibilities are listed after a description of the activity or task.

Phase 1: Organize Project Management Office

Given the State's tight time and budget constraints, considerable effort will be expended in planning, preparing for, and coordinating assessment activities in order to maximize efficiency and the value derived from the assessment effort. The team primarily responsible for these planning and oversight activities is the Project Management Office. As previously noted, the Project Management Office is staffed by a combination of State ITS security professionals and Gartner project management and security assessment subject matter experts.

The tasks and time frames associated with the Phase 1 are depicted in Figure 5.

Figure 5. Phase 1 – Organize PMO Schedule



ID	Task Name
1	**Phase 1 - Organize Project Management Office**
2	**Step 1 - Prepare Tools and Processes**
3	1.1.1 - Prepare Kick-off Meeting Materials
4	1.1.2 - Project KOM
5	1.2 - Prepare Requirements
6	1.3 - Prepare Security Assessment Tool
7	1.4 - Develop Assessment Scorecard
8	1.5 - Develop Vendor Progress Report Templates
9	1.6 - Develop Project Progress Report Template
10	1.7.1 - Develop Assessment Cost Estimates
11	1.7.2 - Finalize Cost Estimates with State
12	1.8 - Develop Deliverable Review and Acceptance Forr
13	**Step 2 - Prepare Agency Assessment Schedule**
14	2.1 - Develop Agency Prioritization Tool
15	2.2 - Perform Prioritization Analysis
16	2.3 - Validate Assessment Schedule with Agencies
17	**Step 3 - Vendor Selection**
18	3.1 - Prepare Vendor Requirements
19	3.2 - Develop Evaluation Criteria and Tools
20	3.3 - Vendor Responses Due
21	3.4.1 - Evaluate Vendor Responses
22	3.4.2 - Vendor Selection Determination
23	3.4.3 - Vendor Approval and Contracting

Step 1: Prepare Tools and Processes

In order to ensure consistent and repeatable assessment processes, and therefore accurate and verifiable assessment results, the Project Management Office will begin by developing the necessary assessment tools and templates. These tools and templates, which will be used by the PMO for project management activities and by vendors during agency assessments, include:

- Project Requirements Document (this document)
- Security Assessment Tool
- Agency Security Assessment Scorecard
- Vendor Project Status Report
- Vendor Billable Activity Report
- Project Status Report and Management Tools
- Communications Plan

- ■ Risk Management Plan
- ■ Detailed Project and Project Work Breakdown Structures (WBS)
- ■ Estimate of Cost for Assessment of Agencies
- ■ Presentations and Communications Tools
- ■ Deliverable Review and Acceptance Form

Gartner subject matter experts will largely be responsible for developing the required tools, templates and processes. ITS will be responsible for review, approval and acceptance of the tools, templates and processes.

PMO Activities and Deliverables

- ❑ Develop the above cataloged project tools and templates and supporting processes.

Vendor Activities and Deliverables

- ❑ None.

Agency Activities and Deliverables

- ❑ None.

Step 2: Prepare Agency Assessment Schedule

The statewide agency security assessment is expected to occur in three waves or groups. Once the number of vendor teams has been determined, the Project Management Office will identify which agencies will be in the first assessment group, and which in subsequent assessment groups. The PMO will then contact each agency to schedule an appropriate time period for required assessment effort. Due to committed budget and project completion schedule, no changes in schedule or budget will be permitted.

PMO Activities and Deliverables

- ❑ Develop an Agency Assessment Prioritization Tool and perform a high-level security risk analysis for assessment prioritization purposes.
- ❑ Create an Agency Group Assessment Schedule.
- ❑ Confirm agency scheduling.

Vendor Activities and Deliverables

- ❑ None.

Agency Activities and Deliverables

- ❑ Notify the PMO of any scheduling conflicts.

Step 3: Vendor Selection

Although the qualification and selection of vendors is largely outside the province of this Requirements Document, it is briefly described here for continuity purposes. The selection process and the results thereof are the sole responsibility of ITS.

As previously noted, the State expects to retain a number of firms to assist in the statewide security assessment effort. Vendors will primarily be selected based upon their expertise and experience. The qualified pool of vendors will then be mapped to agency assignments, with particular attention paid to assigning vendors with experience in special areas of security to those agency with corresponding security needs (i.e., HIPAA, etc.).

PMO Activities and Deliverables

- ❑ Match vendor teams to agencies.

Vendor Activities and Deliverables

- ❑ None.

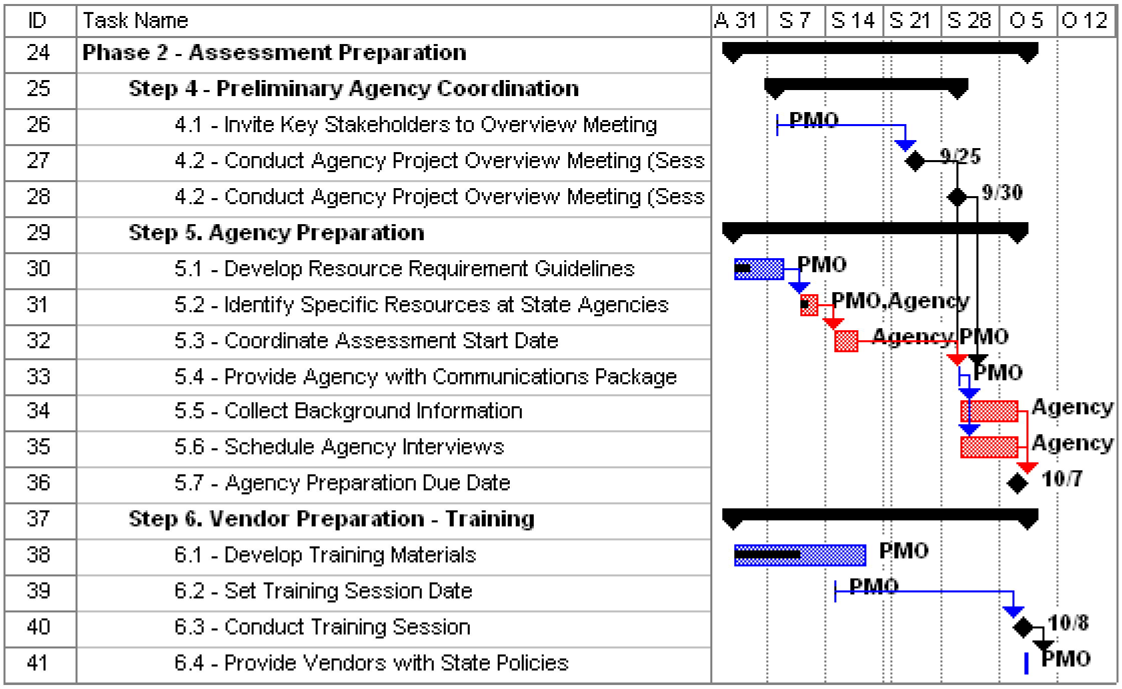
Agency Activities and Deliverables

- ❑ None.

Phase 2: Assessment Preparation

The Assessment Preparation Phase includes all tasks in preparation for the assessments. These tasks are performed only once. The tasks and time frames associated with the Assessment Preparation Phase are depicted in Figure 6.

Figure 6. Phase 2 - Assessment Preparation Schedule



ID	Task Name
24	**Phase 2 - Assessment Preparation**
25	**Step 4 - Preliminary Agency Coordination**
26	4.1 - Invite Key Stakeholders to Overview Meeting
27	4.2 - Conduct Agency Project Overview Meeting (Sess
28	4.2 - Conduct Agency Project Overview Meeting (Sess
29	**Step 5. Agency Preparation**
30	5.1 - Develop Resource Requirement Guidelines
31	5.2 - Identify Specific Resources at State Agencies
32	5.3 - Coordinate Assessment Start Date
33	5.4 - Provide Agency with Communications Package
34	5.5 - Collect Background Information
35	5.6 - Schedule Agency Interviews
36	5.7 - Agency Preparation Due Date
37	**Step 6. Vendor Preparation - Training**
38	6.1 - Develop Training Materials
39	6.2 - Set Training Session Date
40	6.3 - Conduct Training Session
41	6.4 - Provide Vendors with State Policies

Step 4: Preliminary Agency Coordination

In preparation for the assessment effort, the PMO will conduct a formal Agency Project Overview Briefing for all interested stakeholders from State agencies. The Overview Briefing will address the following topics:

- Project Goals and Objectives
- Assessment Process Overview
- Agency Resource Requirements
- Agency Preparation Requirements
- Communications
- Project Schedule and Timeline
- Agency Questions and Concerns.

Proper agency preparation is absolutely critical to the success of the assessment effort. Therefore, the security liaison or his/her designate from each agency will be required to attend the overview meeting. In order to ensure 100% attendance at this mandatory event, two Agency Project Overview Briefing sessions will be held at dates and times noted in Appendix B. Additional agency representatives are encouraged to attend. Vendors are not invited.

PMO Activities and Deliverables

- ❑ Develop Agency Project Overview Briefing presentation materials, invite attendees, and conduct two two-hour Project Overview Meetings.

Vendor Activities and Deliverables

- ❑ Not required – Vendors will not be reimbursed for time or expense incurred. Meeting topics will be addressed with vendors in the formal training sessions described below.

Agency Activities and Deliverables

- ❑ The security liaison or their designated representative from each agency is required to attend. Additional senior management and IT staff from each agency are highly encouraged to attend.

Step 5: Agency Preparation

Although vendor teams will lead the security assessment, the actual process of conducting the security assessment will draw heavily upon agency resources. Agencies must, therefore, be prepared to dedicate or make the appropriate resources available to vendors. Given the State's budget and time constraints, it is imperative that agencies are prepared.

The Project Management Office will send a preparation communications package to agencies being assessed. The agency preparation package will describe the process, agency resource and preparation requirements, assessment schedule, etc. The preparation package will also include a copy of the assessment templates and tools. The agency will be asked to gather required background information and to identify the individuals necessary to support the assessment. The agency will also be required to schedule all essential interviews in the allotted time periods.

Background information as well as the completed interview schedule must be submitted by the agency to the PMO at least one week in advance of the assessment commencement date for that agency. The PMO will review submitted materials for completeness and will forward them to the vendor team designated to conduct the assessment of that agency.

Due to budget and time constraints, it is imperative that agencies make every effort to provide requested information in a timely fashion. Failure of an Agency to complete the requested preparation on time will not be permitted to endanger the project schedule and budget. In order to account for all potential risks the Project Management Office will default all incomplete assessments to the lowest security assessment score.

PMO Activities and Deliverables

- ❑ Develop the Agency Preparation Communications Package.
- ❑ Coordinate assessment start dates with agencies.
- ❑ Track agency compliance and review preparation materials for completeness.

Vendor Activities and Deliverables

- ❑ None.

Agency Activities and Deliverables

- ❑ Review Agency Preparation Communications Package and complete preparation activities including interview scheduling and preliminary data collection.
- ❑ Forward completed interview schedule and required background materials to the PMO at least one week in advance of the scheduled assessment start-date.

Step 6: Vendor Preparation – Training

Vendors will participate in a one-half day training session provided by the Project Management Office. The training session shall provide vendors with the following information:

- Project Goals and Objectives
- Assessment Process Overview
- Agency Support Requirements
- Assessment Tool Familiarization
- Communications and Reporting Requirements
- Reporting Template Familiarization
- State Security Policies Overview
- Project Schedule and Timeline
- Agency Assignments
- Change Management Processes
- State Policy Compliance.

Training is intended to provide vendors with the knowledge necessary to properly record findings using the assessment tools and templates, and to comply with reporting requirements specific to the State's assessment project. Training is not intended to tutor vendors regarding acceptable security practices – vendors are expected to come equipped with the requisite expertise and experience.

PMO Activities and Deliverables

- Develop training materials and conduct a training session that lasts approximately 2-4 hours.
- Provide vendors with copies of applicable State Security Policies.

Vendor Activities and Deliverables

- All vendor team members that will perform or directly support security assessment activities for the State of North Carolina must attend the mandatory training session. Failure to attend the compulsory training will bar affected vendor personnel from participating in the project.
- The State has authorized a total budget of eight (8) person-hours per vendor to attend the training session. While vendors may send additional personnel (within reason) to the training session, the State will not compensate any vendor for more than eight (8) total person-hours.

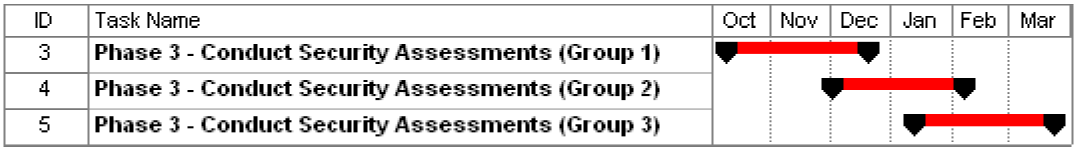
Agency Activities and Deliverables

- None.

Phase 3: Conduct Agency Security Assessments (Per Agency Assigned)

This phase includes tasks associated with the actual assessment of individual agencies. Because more than one round of assessments is needed due to resource constraints, tasks in this phase shall be repeated as required to complete all agency assessment groups. The overall timeline associated with the three assessment rounds is shown in Figure 7.

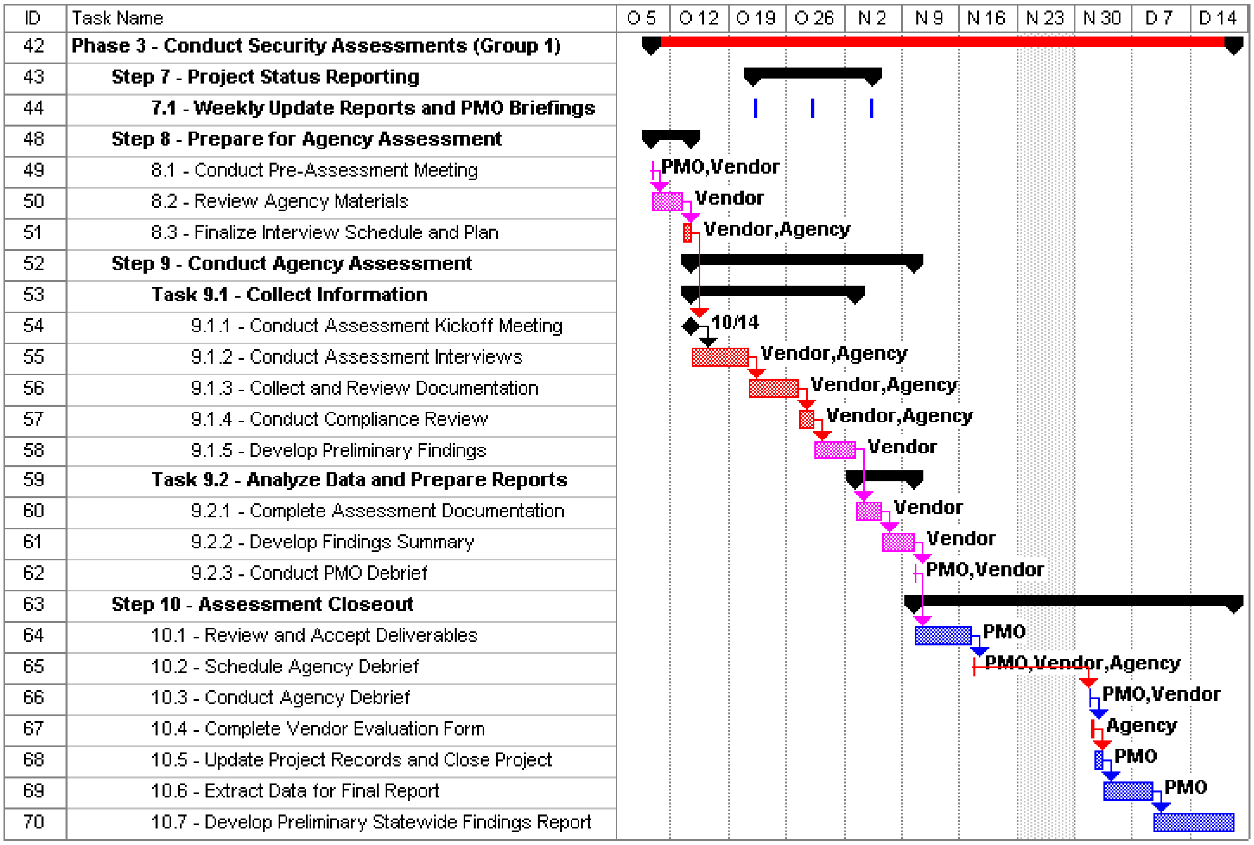
Figure 7. Phase 3 – Security Assessment Groups Schedule



ID	Task Name	Oct	Nov	Dec	Jan	Feb	Mar
3	**Phase 3 - Conduct Security Assessments (Group 1)**	🟥	🟥	🟥			
4	**Phase 3 - Conduct Security Assessments (Group 2)**			🟥	🟥	🟥	
5	**Phase 3 - Conduct Security Assessments (Group 3)**				🟥	🟥	🟥

As previously noted, the State expects that a number of vendor teams will be working in parallel to review the Executive Branch agencies. Teams that demonstrate the appropriate expertise, attention to detail and project management discipline will likely be asked to perform assessments for additional agencies. The State does not expect more than one vendor team to be involved with the assessment of a single agency, nor does the State expect a single team to conduct more that one assessment concurrently. For each agency assigned, the vendor will follow the preliminary project plan depicted below. The task duration depicted will vary based upon the size and complexity of the assessed agency.

Figure 8. Phase 3 – Security Assessment Schedule for Group 1



ID	Task Name
42	**Phase 3 - Conduct Security Assessments (Group 1)**
43	**Step 7 - Project Status Reporting**
44	**7.1 - Weekly Update Reports and PMO Briefings**
48	**Step 8 - Prepare for Agency Assessment**
49	8.1 - Conduct Pre-Assessment Meeting
50	8.2 - Review Agency Materials
51	8.3 - Finalize Interview Schedule and Plan
52	**Step 9 - Conduct Agency Assessment**
53	**Task 9.1 - Collect Information**
54	9.1.1 - Conduct Assessment Kickoff Meeting
55	9.1.2 - Conduct Assessment Interviews
56	9.1.3 - Collect and Review Documentation
57	9.1.4 - Conduct Compliance Review
58	9.1.5 - Develop Preliminary Findings
59	**Task 9.2 - Analyze Data and Prepare Reports**
60	9.2.1 - Complete Assessment Documentation
61	9.2.2 - Develop Findings Summary
62	9.2.3 - Conduct PMO Debrief
63	**Step 10 - Assessment Closeout**
64	10.1 - Review and Accept Deliverables
65	10.2 - Schedule Agency Debrief
66	10.3 - Conduct Agency Debrief
67	10.4 - Complete Vendor Evaluation Form
68	10.5 - Update Project Records and Close Project
69	10.6 - Extract Data for Final Report
70	10.7 - Develop Preliminary Statewide Findings Report

Step 7: Project Status Reporting

In order to ensure an orderly assessment of all agencies, each vendor will be required to provide regular reports to the PMO on project progress, open tasks, emergent issues, preliminary assessment findings, etc. The vendor must complete the required status reports on a weekly basis and send them to the Project Management Office. The PMO will establish a time for a standing weekly meeting with each team during which the vendor project manager will provide a short verbal debrief (30 minutes or less) of the week's activities, open tasks, findings, etc. Documentation relevant to the standing meeting shall be submitted electronically by the vendor to the PMO no later than one hour prior to the weekly status meeting and shall include but not limited to the following:

- Weekly Status Report
- Open Task Report
- Open Issues Report

- ■ Project Performance Report.

Templates for all reports shall be provided by the PMO to each vendor. Appendix E provides some examples of reporting templates. Submission information will be provided.

The vendor must refer all contractual problems via e-mail to the PMO. The e-mail contact information is provided in Appendix F of this document. All vendor work will be conducted on a fixed price basis. The PMO will not revise project scope or budget. Additionally, the vendor will be primarily responsible to work with agencies to resolve problems as they occur. The PMO should be kept abreast of salient developments. All unresolved issues will be referred to ITS management.

To the extent practical, the vendor will be given reasonable and sufficient notice of meeting dates, times and locations. Face to face meetings are required for Kickoff and Debrief Meetings and are preferred for status update meetings. However, the vendor may propose a conference call update meeting, as events require.

PMO Activities and Deliverables

- ❑ Provide project management and reporting tools.
- ❑ Set schedule and participate in weekly project status meetings.

Vendor Activities and Deliverables

- ❑ Submit project reporting tools on a weekly basis and as required.
- ❑ Conduct weekly project status meetings.

Agency Activities and Deliverables

- ❑ None.

Step 8: Prepare for Agency Assessment

Approximately one week prior to the commencement of an assessment for a given agency, the PMO will meet with the assigned vendor to provide an overview of the agency, review the preliminary project plan, and jointly determine if site visits outside of the Raleigh area are necessary. The PMO will provide the vendor with the agency's background materials, contact lists, and interview schedule. After this preparation and hand-off meeting, the vendor will assume responsibility for additional communications and coordination with the agency, and shall be required to finalize the interview schedule, the project plan, and set milestone dates.

PMO Activities and Deliverables

- Conduct one-hour pre-assessment meeting with vendor at the PMO office.
- Provide vendor with agency background information, contact lists, interview schedule and preliminary project plan.

Vendor Activities and Deliverables

- Attend the pre-assessment meeting.
- Review agency materials.
- Coordinate with the agency to finalize the interview schedule and project plan including tasks, schedule, milestones, etc.

Agency Activities and Deliverables

- Coordinate with the vendor team to finalize the interview schedule and project plan.
- Gather information for vendor.

Step 9: Conduct Agency Assessment

Task 9.1: Collect Information

The vendor team will conduct a full assessment of the agency's security posture according to the structure provided by the PMO. In order to ensure that the key security stakeholders (security managers, technologists, business managers, etc.) within the agency are informed of and aligned with the assessment process, the vendor shall begin each agency assessment with a one-hour Assessment Kickoff Meeting. The PMO will provide the vendor with presentation materials for the Kickoff Meeting and a representative of the PMO shall be in attendance at all Kickoff Meetings. Following the Kickoff Meeting, the vendor team will collect the necessary information via interviews, documentation review, and a limited eyes-on compliance review.

The PMO will provide assessment templates and tools and offer guidelines as to the level of sampling and data collection necessary, but vendors will be expected to rely upon their experience and expertise in collecting sufficient data to ensure the accuracy and thoroughness of the agency's assessment. In particular, vendors are advised that agency-specific technologies may not be directly addressed by the assessment tools and templates (for instance, public safety mobile data computer networks). Vendors are required to apply their expertise with such technologies to ensure a complete assessment.

In some instances, the PMO, in conjunction with the vendor, may determine that site visits outside of Raleigh are required to conduct a complete assessment. In such cases, the State shall provide transportation. The State does not expect any travel associated with the security assessment project to require overnight stays outside of Raleigh.

Additionally, in rare instances, upon analyzing the data, the vendor may be required to re-visit an agency or collect more information to document the level of agency compliance with security policies, procedures, and standards. In such circumstances, the vendor must address the gaps within the allocated budget and schedule. Deviation from project schedule or budget is not acceptable.

PMO Activities and Deliverables

- ❑ Provide assessment tools and templates.
- ❑ Attend the agency Assessment Kickoff Meeting.

Vendor Activities and Deliverables

- ❑ Conduct agency Assessment Kickoff Meeting.
- ❑ Conduct Interviews.
- ❑ Collect and Review Documentation.
- ❑ Prepare preliminary assessment.
- ❑ Determine if additional data is required.
- ❑ Conduct Site Visits (as defined in the project plan).

Agency Activities and Deliverables

- ❑ Provide a suitable space for and invite key agency security stakeholders to the Kickoff Meeting.
- ❑ Provide the resources required to facilitate the vendor's assessment efforts, including access to personnel, documentation and equipment, and secure meeting space(s).
- ❑ Provide requested information on a timely basis.

Task 9.2: Analyze Data and Prepare Reports

During this task, the vendor will analyze and document findings from the discovery process completed in the previous task including: review of agency security policies and procedures, background materials, interview notes, etc. The vendor shall complete the assessment tools and templates, and shall develop a Security Assessment Findings Overview in executive summary format (three to six pages, with findings expressed, to the extent possible, in lay terms). The Findings Overview shall focus on identifying key areas of business risk associated with agency security practices.

Vendors will not be required to identify or quantify costs associated with alternatives for remediation, but rather, in areas where risks are identified, they will be expected to provide enough information for the PMO to determine alternatives for remediation and costing. This detailed information will be conveyed to the PMO in the following forms:

- In writing via the required reports
- Via the submission of data and documentation collected from the agencies in support of specific findings or in support of the “current state” to enable the PMO to develop recommendations, and
- In a briefing session at the completion of every assessment.

The PMO Debrief Meeting will also be used as an opportunity for vendors to provide feedback to the PMO regarding general process improvement and recommended template and tool changes.

PMO Activities and Deliverables

- ❑ Schedule and participate in PMO Debrief Meeting.
- ❑ Review deliverables, identify gaps, and provide feedback to vendor for correction.
- ❑ Update processes and tools, as appropriate, based upon vendor feedback.

Vendor Activities and Deliverables

- ❑ Complete assessment documentation.
- ❑ Develop an executive summary Security Assessment Findings Overview.
- ❑ Conduct PMO Debrief Meeting.

Agency Activities and Deliverables

- ❑ None.

Step 10: Agency Assessment Closeout

At the completion of every assessment, the vendor team, a representative(s) from the PMO and designated management personnel from ITS will meet with the assessed agency to debrief the vendor’s findings and conclusions. Prior to debriefing the agency, the vendor’s findings and documentation will be reviewed by the PMO and ITS management personnel for accuracy and completeness. Only after assessment deliverables have been reviewed and accepted by the State will the Agency Debrief be scheduled.

The purposes of the Agency Debrief Meetings are: 1) to provide immediate feedback to agencies regarding their highest risk areas; and, 2) to improve the process for subsequent agencies. The State expects the deliverables review process to take approximately one week. Unless significant issues arise in the deliverables validation and review process, the Agency Debrief is anticipated to occur approximately two weeks after completion of the assessment. Agency Debrief Meetings are planned to last two hours, will be led by the vendor, and should focus on reviewing the highest areas of agency risk.

At the completion of the Debrief, the vendor will submit all interim and final deliverables to the Project Management Office for placement in the Project library. Additionally, at that time, the agency will be asked to complete a Vendor Evaluation Form provided by the PMO. The Evaluation Form will be used for continuous improvement purposes and may be used to assess vendor performance.

PMO Activities and Deliverables

- ❑ Review deliverables for final acceptance. Coordinate ITS review process of deliverables.
- ❑ Update Project Library with all final deliverables in electronic form with one hard copy.
- ❑ Lead the vendor Agency Debrief Meeting.
- ❑ Provide agency with Vendor Evaluation Form and review evaluation feedback.

Vendor Activities and Deliverables

- ❑ Provide all final deliverables in electronic form with one hard copy.
- ❑ Address issues, comments, questions and concerns identified in the PMO deliverables review.
- ❑ Present findings at Agency Debrief meeting.

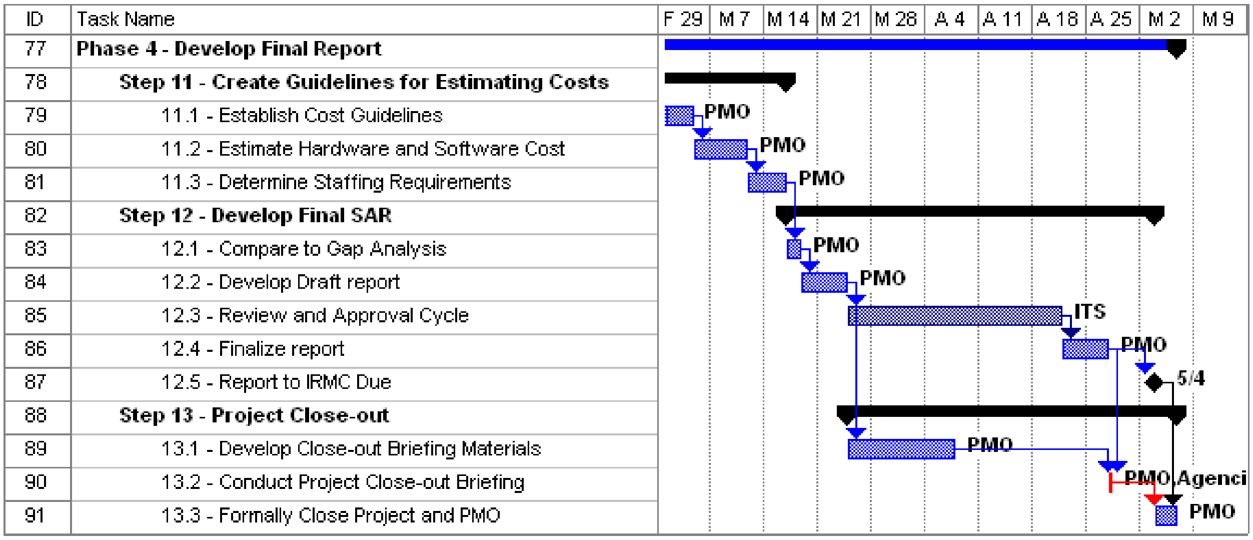
Agency Activities and Deliverables

- ❑ Provide a suitable space for and invite key agency security stakeholders to the vendor Agency Debrief Meeting.
- ❑ Complete the Vendor Evaluation Form and submit to the PMO.

Phase 4: Develop Final Report

This phase includes tasks associated with preparing the final Security Assessment Report (SAR) for the IRMC. Although the schedule below only represents the work effort associated with finalization of the Security Assessment Report after completion of the last group of agency assessments, initial data collation and analysis will begin at completion of the first round of assessments.

Figure 9. Phase 4 – Develop Final Report Schedule



ID	Task Name
77	**Phase 4 - Develop Final Report**
78	**Step 11 - Create Guidelines for Estimating Costs**
79	11.1 - Establish Cost Guidelines
80	11.2 - Estimate Hardware and Software Cost
81	11.3 - Determine Staffing Requirements
82	**Step 12 - Develop Final SAR**
83	12.1 - Compare to Gap Analysis
84	12.2 - Develop Draft report
85	12.3 - Review and Approval Cycle
86	12.4 - Finalize report
87	12.5 - Report to IRMC Due
88	**Step 13 - Project Close-out**
89	13.1 - Develop Close-out Briefing Materials
90	13.2 - Conduct Project Close-out Briefing
91	13.3 - Formally Close Project and PMO

Step 11: Create Guidelines for Estimating Cost

During the course of the findings review process for each assessment group, the Project Management Office will collect, categorize, and prioritize the major security risk issues identified by vendors. This information will be used to: 1) identify any common statewide security risks that require a global remediation approach; 2) help the State to identify and prioritize salient risk exposures; and, 3) develop a preliminary cost and resource estimate for statewide corrective action. The PMO team will then work on guidelines to develop the potential cost of security risk mitigation measures, and will develop recommendations given the risk, exposure, and estimated cost to mitigate the risk.

PMO Activities and Deliverables

- ❑ Collect, categorize and provide preliminary prioritization of vendor-identified security risks.
- ❑ Develop Cost Guidelines for Estimating Cost.
- ❑ Provide corrective action priority recommendations.

Vendor Activities and Deliverables

- ❑ Address any follow-on questions or clarification requests identified by PMO.

Agency Activities and Deliverables

- ❑ None.

Step 12: Develop Final Security Assessment Report (SAR)

During this step, Gartner will produce a Security Assessment Report that will include:

- An executive summary
  - An overview of the assessment process and project status
  - Key findings including recommendations for State remediation priorities
  - Statewide security assessment scorecard
- A planning-level estimate of additional funding needed to bring agencies into compliance
- Identification of security areas where resources can be leveraged to deliver a statewide enterprise security strategy

The final security assessment report will also include key extracts from agency assessment reports including:

  - Assessment of the ability of each agency to comply with the current security enterprise-wide set of standards
  - The rate of compliance with the standards in each agency
  - An assessment of each agency's security organization, network security architecture, and current expenditures for information technology security

The report will be prepared at a level of detail suitable for public consumption in order to avoid compromising agency security. The public report will not contain details sufficient to expose or endanger agency security procedures.

PMO Activities and Deliverables

- ❑ Develop SAR and revise per ITS feedback.

Vendor Activities and Deliverables

- ❑ None.

Agency Activities and Deliverables

- ❑ None.

Step 13: Project Closeout

At the completion of the final report, Gartner will conduct a half-day presentation and workshop. This workshop will provide key agency stakeholders with the opportunity to discuss study findings, conclusions and recommendations.

List of Appendices

Appendix A - Scope Overview Matrix

	100: Info Security Program Charter	**110:** Security Policy	**120:** Organizational Security	**130:** Asset ID & Classification	**140:** Personnel Security	**150:** Physical & Enviro Security	**160:** Comms & Ops Management	**170:** Access Control	**180:** Systems Dev & Maintenance	**190:** Business Continuity Mgmt	**200:** Compliance
People											
Agency / IT Management	◆	◆	◆		◆	◆	◆			◆	◆
Insourced	◆	◆	◆		◆	◆	◆			◆	◆
Outsourced Services (e.g. off site)	◆	◆	◆		◆	◆	◆			◆	◆
Out-tasked Services (e.g. on site)	◆	◆	◆		◆	◆	◆			◆	◆
Hardware											
Mainframe		◆		◆		◆		◆	◆	◆	◆
Midrange		◆		◆		◆		◆	◆	◆	◆
NAS / SAN		◆		◆		◆		◆	◆	◆	◆
Desktops		◆		◆		◆		◆	◆	◆	◆
Laptops		◆		◆		◆		◆	◆	◆	◆
PDAs		◆		◆							◆
Networks											
WAN		◆		◆		◆		◆	◆	◆	◆
LAN		◆		◆		◆		◆	◆	◆	◆
Internet		◆		◆		◆		◆	◆		◆
Intranet		◆				◆		◆	◆		◆
Remote Access		◆				◆		◆	◆		◆
Public Wireless		◆		◆		◆		◆	◆		◆
Mobile Data and Voice Radio		◆									
Voice											
PBX / Key Systems		◆		◆		◆		◆	◆	◆	◆
Voice Mail		◆		◆		◆		◆	◆	◆	◆
Cell Phones/Pagers		◆									
Software Infrastructure											
Middleware (including transport)		◆		◆				◆	◆	◆	◆
DBMS		◆		◆				◆	◆	◆	◆
Web Services / Portals		◆		◆				◆	◆	◆	◆
Workgroup Computing		◆		◆				◆	◆	◆	◆
Virus Protection		◆		◆				◆	◆	◆	◆
Firewalls		◆		◆				◆	◆	◆	◆
Other Utilities		◆									
Application Software											
Back Office (Finc, HR, etc.)		◆	◆	◆		◆		◆	◆	◆	◆
Front Office (Agency Specific Apps)		◆		◆		◆		◆	◆	◆	◆
Other COTS Business Applications		◆		◆		◆		◆	◆	◆	◆
Other Custom Business Apps		◆		◆		◆		◆	◆	◆	◆
Business Intelligence / DW		◆		◆		◆		◆	◆	◆	◆
Integrated Document Management		◆		◆		◆		◆	◆	◆	◆

◆ denotes included in scope

Appendix B - Project Key Activity Dates and Deadlines

Activity/Deadline	Date	Notes
Vendor Bid Responses Due	Sept 3	Completed
Vendor Selection Complete	Sept 15	Completed
Agency Project Overview Briefing (Session 1)	Sept 25	1:30 pm – 3:30 pm Department of Cultural Resources Auditorium
Agency Project Overview Briefing (Session 2)	Sept 30	2:00 pm – 4:00 pm Department of Cultural Resources Auditorium
Vendor Assessment Training	Oct 8	1:00 pm – 5:00 pm Department of Cultural Resources Auditorium
Agency Assessment Kick-Off - Group 1	Oct 13	At Agency location
Agency Assessment Kick-Off - Group 2	Dec 2	At Agency location
Agency Assessment Kick-Off - Group 3A	Jan 12	At Agency location
Agency Assessment Kick-Off - Group 3B	Jan 28	At Agency location
Security Assessment Report Due	May 4	

Appendix C – Vendor Work Effort Breakdown

	Task Duration (calendar hours)		
Activities per Agency	***Type 1***	***Type 2***	***Type 3***
Step 7. Project Status Reporting			
7.1 Prepare Weekly Update Reports	3	3	3
7.1 Conduct Weekly PMO Status Meeting	2	2	2
Step 8. Prepare for Agency Assessment			
8.1 Conduct Pre-Assessment Meeting	1	1	1
8.2 Review Agency Materials	4	8	16
8.3 Finalize Interview Schedule and Plan	2	2	2
Step 9. Conduct Agency Assessment			
Task 9.1. Collect Information			
9.1.1 Conduct Assessment Kickoff Meeting	1	1	1
9.1.2 Conduct Assessment Interviews	16	24	40
9.1.3 Collect and Review Documentation	22	40	50
9.1.4 Conduct Compliance Review	4	8	16
9.1.5 Develop Preliminary Findings	8	12	16
Task 9.2. Analyze Data and Prepare Reports			
9.2.1 Complete Assessment Documentation	16	28	32
9.2.2 Develop Findings Summary	4	4	4
9.2.3 Conduct PMO Debrief / Revisions	14	14	14
Step 10. Assessment Closeout			
10.2 Schedule Agency Debrief	1	1	1
10.3 Conduct Agency Debrief	2	2	2
Total duration per category (calendar hours)	100	150	200
Size of Team (persons per task*)	2	2	2
Person-Hours to Complete Assessment	200	300	400
(* vendors may choose to use more staff; hours are fixed)			

Appendix D – Non-Disclosure Agreement and Background Check Form

State of North Carolina
Office of Information Technology Services

Michael F. Easley, Governor **George Bakolia, State Chief Information Officer**

Non-Disclosure Agreement
For
ITS and Other Government Employees and Third-Party Providers[1]

I have read this agreement and I agree to comply fully with the following terms and conditions.

As an ITS employee, an employee of another government agency, or as a Third-Party Provider to ITS or another government agency, I agree that signing this Non-Disclosure Agreement and fully complying with all the terms and conditions are requirements for working at ITS. Further, compliance with this agreement by a Third Party Provider is material to the performance of the contract between ITS and the Third-Party Provider or the other government agency and its Third Party Provider.

1. ITS holds government records of other agencies for the purposes of storage or safekeeping or to provide data processing. For purposes of the Public Records Law, ITS is not a custodian of any records generated on behalf of another agency.

2. Only a custodian of records can decide when records can be made public. A custodian of records is a public official in charge of the government agency that generated the records. Only public officials or their designees are authorized to release records to the public. Neither an ITS employee nor a Third Party Provider is authorized to release government records of other agencies. Employees of other government agencies and their contractors must comply with both this requirement and their specific agency's requirements, as applicable.

3. Information that belongs to agencies may include highly sensitive and confidential data. In many instances, improper release or use of other agency information by an ITS or other government employee or Third Party Provider is a crime.

4. ITS employees and Third Party Providers also have no authority to determine whether a record is public or not. Only the agencies that store their records with ITS can make that determination for their records and only the management at ITS can make that determination for ITS records.

5. **ITS employees and Third Party Providers are not permitted to release records or information contained in records that belong to other agencies. Requests for such information must be channeled through the ITS supervisor to the ITS Public Information Officer for action according to ITS policy. Employees of other government agencies and their contractors must comply with both this requirement and their specific agency's requirements, as applicable.**

6. SPECIAL PROVISION. TAX INFORMATION. As part of my duties as an ITS or other government employee or third-party provider and as required by statute, I may be performing tasks involving use or storage of confidential state and federal tax information. As such an employee or third party provider, I may be subject to substantial civil and criminal penalties imposed by various state and federal statutes (North Carolina G.S. §105-259 and the Internal Revenue Code, 26 U.S.C. §§6103, 7213, 7213A, 7413) for unauthorized disclosure or inspection of tax information. Moreover, I may be requested by other persons to provide access to tax data. Because this may be a violation of the statutes cited above, I agree to seek authorization from appropriate Department of Revenue officials before granting access to tax records to other individuals.

[1] Third party providers are non-state employees, such as vendors, suppliers, individuals, contractors, and consultants, including their employees and agents, responsible for providing goods or services to the state. In order to perform the requested services, a third party may require access to information technology assets and access to agency information determined to be valuable to operations and/or classified as confidential by law.
Q:\ISO\WORKGRP\White\Policies\revised non disclosure.doc

7. SPECIAL PROVISION. PERSONALLY IDENTIFIABLE HEALTH INFORMATION. As part of my duties as an ITS or other government employee or third-party provider and as required by statute, I may be performing tasks involving use or storage of confidential state and federal personally identifiable health information that is protected from disclosure under federal rules adopted under the Health Insurance and Accountability Act of 1996 and state law. As such an employee or third party provider, I acknowledge and agree that I may be subject to substantial civil and criminal penalties imposed by various state and federal statutes (including but not limited to North Carolina G.S. §122C-52 and the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 104th Congress) for unauthorized disclosure or inspection of personally identifiable health information as well as personnel disciplinary action. Moreover, I may be requested by other persons to provide access to this health data. Because this may be a violation of the statutes cited above, I agree to seek authorization from appropriate agency officials before granting access to health records to other individuals.

8. SPECIAL PROVISION. CRIMINAL JUSTICE INFORMATION. As part of my duties as an ITS or other government employee or third-party provider and as required by statute, I may be performing tasks involving use or storage of confidential state and federal criminal records information. As such an employee or third party provider, I acknowledge and agree that I may be subject to civil penalties imposed by federal Privacy Act of 1974, 5 U.S.C. § 552a, as amended, for unauthorized disclosure or inspection of criminal record information as well as personnel disciplinary action. Moreover, I may be requested by other persons to provide access to the criminal record information. I agree to seek authorization from appropriate agency officials before granting access to criminal records information.

Because of the above restrictions on use of information stored at ITS, I agree not to release any information that I access at ITS without proper authority or permission. I further agree not to discuss information obtained from the databases and not to use the databases except in compliance with the Office of Information Technology Services Policy Manual or, if I am an employee of another government agency, in compliance with that agency's requirements, as applicable.

As an ITS or other government agency employee, I acknowledge and agree that failure to comply with the non-disclosure agreement may result in personnel action. As a Third Party Provider, I acknowledge and agree that failure to comply with this non-disclosure agreement may be considered a material breach of the contract and will result in denial of access to information at ITS. As stated above, in some instances failure to comply with the non-disclosure agreement may subject me to criminal prosecution.

AGREED, this _____ day of _________, 200_. I also acknowledge that I have been provided a copy of this agreement.

________________________________	________________________________
Employee Name Printed	Employee of Third Party Name Printed
________________________________	________________________________
Employee Signature	Employee of Third Party Provider Signature
Division/Agency: ____________________	Company Name:______________________

Statutory Authority: N.C. §132-2

cc: ITS Information Security Office
cc: Signatory

CRIMINAL BACKGROUND CHECK AUTHORIZATION FORM

NOTIFICATION AND RELEASE
ITS CONTRACTOR

I hereby acknowledge that I have been informed by ITS that ITS will obtain a criminal background check as a result of ITS policy. The Personnel Office will administer the criminal background check program in a confidential manner. The results of criminal background checks will be provided to authorized individuals only. I acknowledge that ITS will inform me if a criminal background check reveals a possible criminal conviction against me. I understand that I may obtain a free copy of the background check.

I certify that if I provide an application for contract work with ITS the information contained therein is true to the best of my knowledge and belief. I understand that any misrepresentation or false statement made by me in the application or any related documents, and which is deemed material by ITS may result in the following actions: ITS may not enter a contract with me or any firm with which I am associated or ITS may terminate the contract. I understand and agree that all information furnished in my application and all attachments may be verified by ITS or its authorized representative. I hereby authorize all individuals and organizations named or referred to in my application, as well as, any law enforcement organization to give ITS all information relative to such verification; hereby release such individual, organization and ITS from any and all liability or claim of damage resulting from such information.

Please list all names that you have used during the last seven (7) years, including married, unmarried and aliases: Please print.

Names (First, Middle, Last):________________________________ Date of Birth mm/dd/yyyy________

Unmarried Name (First, Middle, Last):_________________________Date Used mm/dd/yyyy__________

Social Security #_______________________Driver's License #_______________________

Current and Previous Address(es) for the past seven years: Please use extra page if necessary

Number and Street____

City, State County Zip____

Number and Street____

City, State, County, Zip____

Number and Street____

City, State, County, Zip____

Contractor signature: _________________________________Date:_____________

Will this individual require physical or logical access to the Criminal Justice Information Network?
______ YES ______ NO If yes, a background check requiring fingerprinting is required and will be arranged by Personnel Services.

Manager signature: ____________________________________Date:______________
Please return completed form to ITS Personnel Office

Appendix E – Example Report Templates

Weekly Status Report

State of North Carolina
Information Resource Management Commission
Agency Security Assessments
Vendor Weekly Project Status Report

A. General Information

Date: September 12, 2003 ***Prepared by:***

Authorized by: ***Modification Date:***

Project is: ☒ **On Plan** ☐ **Ahead of Plan** ☐ **Behind Plan**

Reporting Period: **From:** August 25, 2003 **To:** September 12, 2003

B. Summary

C. Current Activity Status

D. Accomplishments for Current Week

E. Planned Activities for Next Week

Project Open Task Report

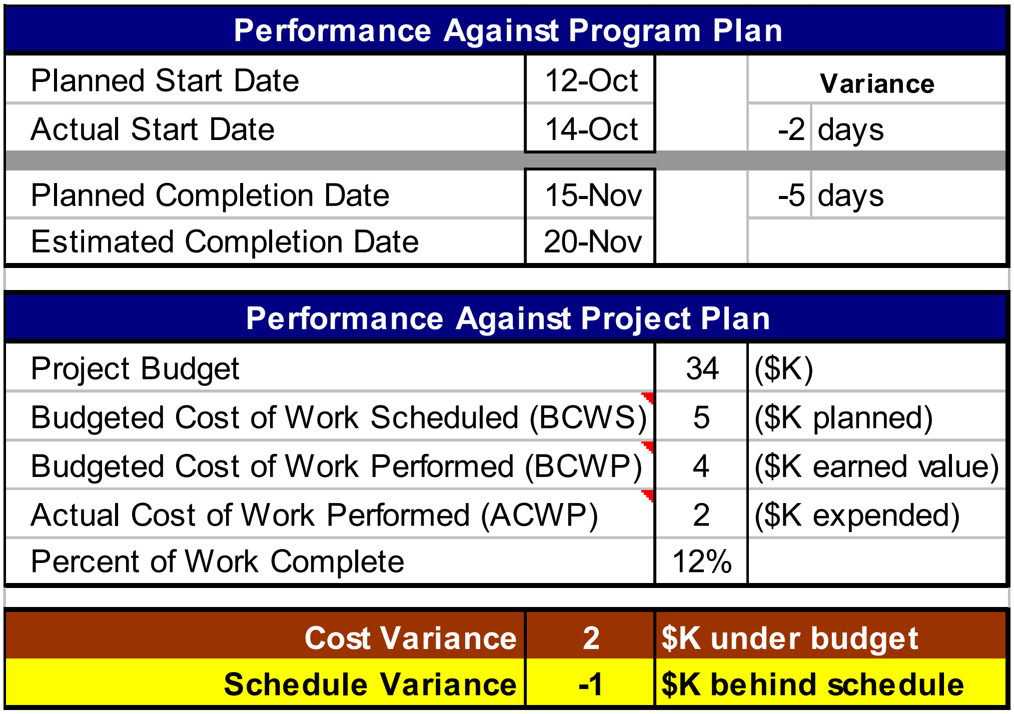
Completed Tasks	
#	Description

Open Tasks		
#	Description	Status

Open Issues Report

Date	Vendor Name	Vendor Contact Name	Priority: Low, Medium, High	Issue Description

Project Performance Report



Performance Against Program Plan				
Planned Start Date	12-Oct		Variance	
Actual Start Date	14-Oct		-2	days
Planned Completion Date	15-Nov		-5	days
Estimated Completion Date	20-Nov			

Performance Against Project Plan		
Project Budget	34	($K)
Budgeted Cost of Work Scheduled (BCWS)	5	($K planned)
Budgeted Cost of Work Performed (BCWP)	4	($K earned value)
Actual Cost of Work Performed (ACWP)	2	($K expended)
Percent of Work Complete	12%	

Cost Variance	**2**	**$K under budget**
Schedule Variance	**-1**	**$K behind schedule**

Appendix F – Important Contact Information

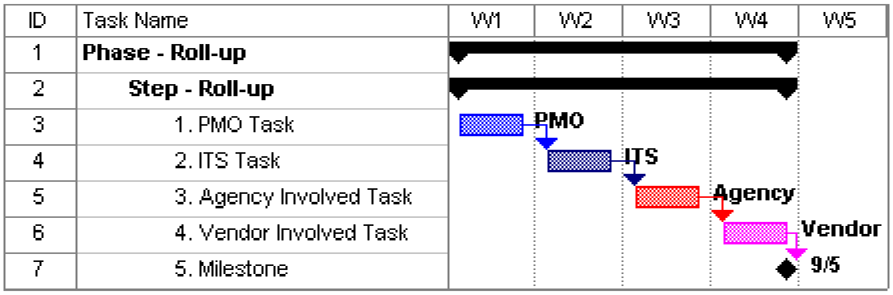
Project Management Office

E-mail:	security.pmo@ncmail.net
Phone:	(919) 850-2187

Appendix G – Glossary of Acronyms

Acronym	Definition
CIO	Chief Information Officer
HIPPA	Health Information Protection and Portability Act
IPPC	Information Protection and Privacy Committee
IRMC	Information Resource Management Commission
PMO	Project Management Office
ISO	International Standards Organization
ITS	Office of Information Technology Services
SAR	Security Assessment Report
SCIO	State Chief Information Officer
WBS	Work Breakdown Structure

Appendix H – WBS Legend



ID	Task Name
1	**Phase - Roll-up**
2	**Step - Roll-up**
3	1. PMO Task
4	2. ITS Task
5	3. Agency Involved Task
6	4. Vendor Involved Task
7	5. Milestone